

21. ((Four Times Amended) A storage medium comprising:

a stored program for execution by a processor wherein the program facilitates providing updated digital signature key pairs in a public key system by:

allowing entry of selectable expiry data for a plurality of clients and not through a client, including both at least public verification key expiry data and signing private key expiry data that are selectable on a per client basis wherein the digital signature key pairs are not shared among users;

digitally storing both selected public key expiry data and selected private key expiry data for association with a new digital signature key pair; and

associating the stored selected expiry data with the new digital signature key pair to affect a transition from an old digital signature key pair to a new digital signature key pair.

REMARKS

Applicants respectfully traverse and request reconsideration.

Claims 1-4, 6, 8-18, 20-24 and 26 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Lewis in view of the Ellison article. Applicants have amended claim 1 to point out that the method is for providing updated digital signature key pairs to a plurality of clients in the public key system and that the multi-client manager unit provides selectable digital signature expiry data and not a client or recipient of a key pair. The selectable digital signature expiry data includes a public verification key expiry data and selectable private signing key

expiry data for a plurality of clients that are selectable on a per client basis when the digital signature key pairs are not shared among users.

It appears that the Lewis reference has been cited for showing a public key replacement system that causes a key switch. Applicants respectfully submit that the Lewis reference teaches a specific type of key replacement system as pointed out in previous responses. The Lewis reference is directed to selecting replacement keys so that it is computationally difficult to determine a replacement key from its masked version. Each time a key request is performed, an active public key is discarded. A key replacement message is signed by an active private key and replacement private key. Accordingly, the message is signed by replacement private key. The Office Action also indicates that Lewis does not say that there are certificates with expiry data that is user selectable. Applicants respectfully note that the claims do not claim user selectable expiry data for certificates. As such, Applicants are uncertain as to the meaning of the statement. Classification would be appreciated.

In addition, Applicants' claim requires providing, by a multi-client manager unit, and not by a client, selectable digital signature expiry data including selectable private signing key expiry data and public verification key expiry data for a plurality of clients, that are selectable on a per client basis and wherein the digital signature key pairs are not shared among users as well as digitally storing both selected public key expiry data and the selected private key expiry data and associating the storage selected expiry data and the new digital signature key pair to effect a transition from the old signature key pair to a new digital signature key pair. Lewis is silent as to all of these limitations. Accordingly, it appears that the Ellison reference must teach all of Applicants' claimed limitations.

Applicants respectfully submit that the cited portion of Ellison in discussing that a user may somehow determine validity periods and that a user should define validity periods according to risk management. The Ellison reference is silent as to how this idea is carried out. Applicants respectfully submit that Ellison does not teach providing, by multi-client manager unit, and not by a client, selectable digital signature expiry data for a plurality of clients that are selectable on a per client basis and when the digital signature key pairs are not shared among users. In addition, the claim requires digitally storing both selected public key expiry data and selected private key expiry data for association with a new digital signature key pair and subsequently associating the stored selected expiry data with a new digital signature key pair to effect the transition from an all digital signature key pair to a new digital signature key pair. Since Lewis doesn't describe these operations, the Ellison reference must describe such a method. However, there is no restrictive multi-client manager unit described nor providing selectable digital signature expiry data for a plurality of clients wherein the data is selectable on a per client basis. Moreover, Ellison does not teach wherein the digital signature key pairs are not shared among users, and digitally storing selected information and associating that information with a new digital signature key pair. Accordingly, Applicants respectfully submit that the claims are in condition for allowance.

Claims 5, 19 and 25 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Lewis and Ellison as applied to claims 1, 14 and 21 above, and further in view of Applicants' admitted prior art. The "Response to Arguments" section of the Office Action states that Applicants previous amendment seemed to create a contradiction by using the words "selectable predetermined percentage". Applicants respectfully submit that the language becomes clear when read in light of the specification. For example, a predetermined percentage may be for

example 50%, 75% or 25% wherein each of these percentages may be selectable through the multi-client manager unit. Accordingly, Applicants respectfully submit that the amended claims are clear in view of the specification. The selectability operation alters the scope of the claims since the claim previously did not require the predetermined percentages to be stored and presented to be selectable. Accordingly, Applicants respectfully reassert the relevant remarks made in the previous Office Action and note that such operations are not taught or suggested by a combination of Lewis, Ellison and Applicants' submitted prior art.

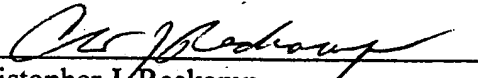
In addition, with respect to the new claims, there does not appear to be a rejection of the claims in the body of the rejection. However, there is a reference to the new claims in the "Response to Argument" section. However, there is no statutory basis for rejection such as whether these claims are rejected under 35 U.S.C. § 103 in view of certain references, or whether the Examiner wishes to reject the claims or using another statutory section or allow the claims. Accordingly, Applicants respectfully submit that a subsequent Office Action should not be made final since the basis for the rejection of the new claims has not been presented in this Office Action. In any event, these claims are believed to be allowable for the same reasons as claims 5, 19 and 25 as well as the independent claims from which they depend.

Attached hereto is a marked-up version of the changes made to Claims 1, 14 and 21 by the current amendment. The attached page is captioned: "Version with Markings to Show Changes Made."

BEST AVAILABLE COPY

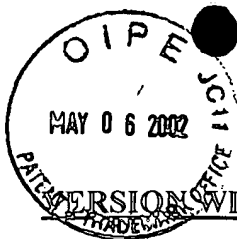
Accordingly, Applicant respectfully submits that the amended claims are in condition for allowance. The Examiner is invited to contact the below-listed attorney if the Examiner believes that a conference would expedite the prosecution of the instant application.

Respectfully submitted,

By: 
Christopher J. Reckamp
Registration No. 34,414

Date: April 25, 2002

VEDDER, PRICE, KAUFMAN &
KAMMHOLZ
222 N. LaSalle Street
Chicago, IL 60601
(312) 609-7599; FAX: (312) 609-5005



COPY OF PAPERS
ORIGINALLY FILED

VERSION WITH MARKINGS TO SHOW CHANGES MADE

Please substitute the below claims 1, 14 and 21 for the indicated pending claim with the same number:

1. (Five Times Amended) A method for providing updated digital signature key pairs to a plurality of clients in a public key system comprising the steps of:

providing, by a multi-client manager unit and not by a client, selectable digital signature expiry data including at least public verification key expiry data, and selectable private signing key expiry data to a plurality of clients, that are selectable on a per client basis wherein the digital signature key pairs are not shared among users;

digitally storing both selected public key expiry data and selected private key expiry data for association with a new digital signature key pair; and

associating the stored selected expiry data with the new digital signature key pair to affect a transition from an old digital signature key pair to a new digital signature key pair.

14. (Four Times Amended) A system for providing updated digital signature key pairs to a plurality of clients in a public key system comprising:

multi-client manager means for providing selectable digital signature expiry data to a plurality of clients and not by a client, including at least both public verification key expiry data and private signing key expiry data that are selectable on a per client basis wherein the digital signature key pairs are not shared among users;

means, accessible by the multi-client manager means, for digitally storing both selected public key expiry data and selected private key expiry data for association with a new digital signature key pair; and

means, responsive to the stored selected public key expiry data, for associating the stored selected expiry data with the new digital signature key pair to affect a transition from an old digital signature key pair to a new digital signature key pair.

21. ((Four Times Amended) A storage medium comprising:

a stored program for execution by a processor wherein the program facilitates providing updated digital signature key pairs in a public key system by:

allowing entry of selectable expiry data for a plurality of clients and not through a client, including both at least public verification key expiry data and signing private key expiry data that are selectable on a per client basis wherein the digital signature key pairs are not shared among users;

digitally storing both selected public key expiry data and selected private key expiry data for association with a new digital signature key pair; and

associating the stored selected expiry data with the new digital signature key pair to affect a transition from an old digital signature key pair to a new digital signature key pair.